

IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF
LINUX PC S/N: PTNB60202200408A4F2700
LOCATED AT HSI MEMPHIS, 775 RIDGE
LAKE BLVD. STE.300, MEMPHIS, TN

Case No. 23-SW-254

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A WARRANT TO
SEARCH AND SEIZE**

I, Benjamin W. Grant, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Homeland Security Investigations (HSI) Special Agent (SA) and have been since January 2017. I am currently assigned to the HSI Assistant Special Agent in Charge (ASAC), Memphis, Tennessee. I completed an intensive six-month academy at the Federal Law Enforcement Training Center, located in Glynco, Georgia, which included the Criminal Investigator Training Program and the HSI Special Agent Training Program. While attending the Federal Law Enforcement Training Center I received training in the investigative areas of customs and immigration fraud, child sexual abuse material, human trafficking, narcotics smuggling, money laundering, bulk cash smuggling, the illegal exportation of weapons, munitions and high technology items, the illegal exportation of commodities, general smuggling, and alien smuggling. Before my employment with HSI, I earned a graduate degree from the University of Scranton and served in the U.S. Air Force.

STATUTORY VIOLATIONS

2. Based upon the information contained in this affidavit, I have probable cause to believe that, located a Linux PC S/N: PTNB60202200408A4F2700 (hereinafter SUSPECT

DEVICE), there is evidence, fruits, and instrumentalities of violations of federal law, namely 18 U.S.C. §§ 2252 and 2252A, possession and distribution of child pornography, as more particularly described in Attachment B.

3. I make this affidavit in support of an application for a warrant to search SUSPECT DEVICE which is in the Western District of Tennessee, described more fully in Attachment A, and to seize the items relating to violations of 18 U.S.C. §§ 2252 and 2252A, as more fully described in Attachment B.

4. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals participating in this investigation, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during this investigation.

DEFINITIONS

5. The below definitions apply to this Affidavit and Attachment B to this Affidavit.

6. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

7. “Visual depictions” includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

8. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

9. “IP Address” means Internet Protocol address, which is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

10. “Internet” means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

11. In this affidavit, the terms “computers” or “digital storage media” or “digital storage devices” may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

BACKGROUND REGARDING PEER-TO-PEER FILE SHARING

12. File sharing is a method of distributing electronically stored information, including digital media such as images and videos. Peer-to-peer (P2P) file-sharing applications enable networks of computer users to share and access files on their computers through the Internet. Participants in a P2P file-sharing network typically designate certain computer files for access by others within their network. Through the Internet, those within the network can then use the P2P file sharing application to obtain designated files and transfer them to their own computer. P2P file sharing applications have proved to be a prolific means for the receipt and distribution of child pornography through the Internet.

13. The IP address is unique to a particular computer during an online session. The IP address can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

14. Third party software is available to identify the IP address of the peer-to-peer computer sending the file and to identify if parts of the file came from one or more IP addresses. Such software monitors and logs Internet and local network traffic.

SEIZURE AND SEARCH OF COMPUTERS

15. As described above and in Attachment B, I submit there is probable cause to search and seize SUSPECT DEVICE for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon

forensic analysis. They may be seized and searched on-scene, and/or searched off-scene in a controlled environment.

16. For example, based on my knowledge, training, and experience, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

17. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

18. Also, based on my training and experience, wholly apart from user-generated files, computer storage media contain electronic evidence of how a computer has been used, what it has

been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, virtual memory “swap” or paging files, and shadow copies of previous versions of systems or files, or paging files. Computer users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted, edited, moved, or show a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

19. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, why they were used, the purpose of their use, and the purposes to which they were put, who used them, the state of mind of the user(s), and when they were used.

20. The monitor and printer are also essential to show the nature and quality of the images or files that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as

all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords, and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

21. The computer and its storage devices, the mouse, the monitor, keyboard, printer, modem, and other system components are also used as instrumentalities of the crime to operate the computer to commit offenses involving the sexual exploitation of minors. Devices such as modems and routers can contain information about dates, IP addresses, MAC addresses, frequency, and computer(s) used to access the Internet or to otherwise commit the crimes described herein. The computer equipment may also have fingerprints on them indicating the user of the computer and its components.

22. Information or files related to the crimes described herein are often obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession, or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

23. “User attribution” evidence can also be found on a computer and is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, videos, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. For example, I know from training and experience that persons trading in, receiving, transporting, distributing, or possessing images involving the sexual exploitation of children or those interested in the firsthand sexual exploitation of children often communicate with others through correspondence or other documents which could tend to identify the origin and possessor of the images as well as provide evidence of a person's interest in child pornography or child sexual exploitation. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

24. Searching computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or Internet use is in various operating system log files that are not easily located or reviewed. Or a person engaged in criminal activity will attempt to conceal evidence of the activity by “hiding” files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical

objects requires searching the entire premises for those objects that are described by a warrant, a search of SUSPECT DEVICE for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use a multitude of techniques, both on and off-scene, including more thorough techniques.

25. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes involving child exploitation, they should all be seized as such.

26. Based on my training and experience, I know that a thorough search for information stored in digital storage media requires a variety of techniques that often includes both on-site seizure and search as well as a more thorough review off-site review in a controlled environment. This variety of techniques is required, and often agents must seize most or all storage media to be searched on-scene and/or later in a controlled environment. These techniques are often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

27. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include off-site techniques since it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined off-site and in a controlled environment. This is true because of the below.

a. The nature of evidence. As noted above, not all evidence takes the form of

documents and files that can be easily viewed on site. Analyzing evidence of how, when, and why a computer has been used, by whom, what it has been used for, requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a “booby-trap”), the controlled environment of a laboratory may be essential to its complete and accurate analysis. Searching for and attempting to recover any deleted, hidden, or encrypted data may be required to determine whether data falls within the list of items to be seized as set forth herein (for example, data that is encrypted and unreadable may not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of child exploitation offenses).

- b. The volume of evidence and time required for an examination. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for

things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.
- e. Need to review evidence over time and to maintain entirety of evidence. I recognize the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit and in Attachment B in order to prevent unnecessary invasion of privacy and overbroad searches. I advise it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single analysis. I have learned through practical experience that various pieces of evidence retrieved from digital devices in investigations of this sort often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered

within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between pieces of an investigation as that investigation continues, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. In the past, I have reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. I have learned from that experience, as well as other investigative efforts, that multiple reviews of the data at different times is necessary to understand the full value of the information contained therein, and to determine whether it is within the scope of the items sought in Attachment B. In order to obtain the full picture and meaning of the data from the information sought in Attachments A and B of this application, the Government would need to maintain access to all of the resultant data, as the completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As such, I respectfully request the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation, rather than

minimize the content to certain communications deemed important at one time. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

28. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for permits both on-site seizing, imaging and searching as well as off-site imaging and searching of storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later and perhaps repeated examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

29. Because this warrant seeks only permission to examine the device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the court to authorize execution of the warrant at any time in the day or night.

INVESTIGATION

30. During November 2022, FBI Task Force Officer John Chevalier was conducting an online investigation which utilized a law enforcement version of a publicly available P2P file-sharing program. This law enforcement version was configured to download suspected child pornography files directly from other computers using the same file sharing protocol. The law enforcement version of the program specifically allows personnel to download files from one

individual user, rather than from multiple users. The law enforcement version of the program cannot download files that are not made available by the suspect.

31. On November 9 and 11, 2022, a computer run by FBI Task Force Officer John Chevalier made direct connections to IP address 76.138.92.28 (SUSPECT DEVICE), which was making files of child pornography available for download through the P2P file-sharing protocol, and downloaded directly from that SUSPECT DEVICE files of child pornography. The download was turned over to HSI.

32. I found that on November 9, 2022, a direct connection was made with SUSPECT DEVICE at IP Address 76.138.92.28 which was the sole candidate for each download, and as such, each file was downloaded directly from this IP address. Eight files were downloaded, noted below.

- a. File name: (Pthc) 4yo Susan.mpg
- b. File name: Stickam 12 Yo White .avi
- c. !! NEW Pthc - 11yo Tara (Tara Part 2).mpg
- d. File name: Irisa (Valya)Part2- 11Yo Totally Dadgirl Pthc-Kinderkutje.avi
- e. File name: (Kingpass) (Hussyfan) (pthc) (r@ygold) (babyshivid) 14yo G.mpg
- f. (Pthc) Lily 10Yo Takes It Fully - 8m39S.avi
- g. 9 yo Blonde In Camping Incest(3m8s)pthc.avi

33. I found that on November 11, 2022, a direct connection was made with SUSPECT DEVICE at IP Address 76.138.92.28 which was the sole candidate for each download, and as such, each file was downloaded directly from this IP address. 21 files were downloaded, noted below.

- a. File name: !New!(Pthc)Niece Series2 (5y Full Penetration) (62m20s).mpg
- b. (Pthc) 6yo Favela Full (1+2) BEAUTIFUL_Very willing angel faced little girl relieved~Kids need sex 2~!.mpg

- c. (Kinderkutje) (Pthc) Hc-c4G--Compile 4 Girls--All Small And Loving It--9.08 9Yo
Mpg 7Yo Girl Try To Fuck Ptsc Hussyfan Kingpass Kleuterkutje.mpg
- d. PTHC -G- CBABY 4yo SPECIAL 4m20s.mpg
- e. awesome preteen compilation 2.mpg
- f. T-83418160-(pthc) Family 2 - ReelFamilySex - entire clip - Hot Mother licks her
8yo Daughters sweet pussy as her brother fucks her - r@ygold - ddoggprn - incest
REELKIDDYMOV.mpg
- g. little girls mix (lolitas-preteens-reelkiddymov-r@ygold-hussyfans-underage-girls-
children-pedofilia-ptsc-xxx-sexy).mpeg
- h. 16Yo Thai Girl With Two Boys, 18Yo And 17Yo Shaved Recomendo Flagras Big
Brotherl.mpg
- i. !!! NEW !!! 2010 kait 5yo - chunk2 FK pthc best.avi
- j. stickam-rack_13yo love-bate1a.avi
- k. PTHC - beauty-cumshot 3yo THIS ROCKS pedo child toddler incest 2yo
4yo 5yo 6yo 7yo 8yo babyj vicky laura jenny sofie fdsa hussyfan russian
korea.mpg
- l. (Pthc) !!! New 0604 !!! Luvnlilly 3Yo(1).avi
- m. Pthc dad try ass but go sex on 10Yo girl.mpg
- n. pthc Pedoland Frifam Toddler Fucking & Cumshots 3yo girl, Very Good!!.mpg
- o. (KINGPASS) NEW! 022 Asian - pthc (tied 8yo Cambodian boom-boom girl
fucked + raped by sex-tourist) hussyfan.mpeg
- p. Kinderficker Pthc Ptsc Hussyfan R@Ygold Kingpass Qqaazz I Fuck My 1.mpg
- q. Pthc Pedoland Frifam 5Yo Old Best Cock Sucker In The World.mpg

- r. PTHC - jenrry_compl_preteens actually fucking.mpg
- s. pthc Pedoland Frifam webcam 12yo Viviane Striptease 2010.avi
- t. (Pthc) 6Yo Babyj - Bedtime Rape .mpg
- u. !!!New!!! Homevid - Dau(7Yo)-1 Pedo Ptsc Kleuterkutje.mpg

34. On December 27, 2022, I learned, via legal process, the internet service subscriber information for SUSPECT DEVICE assigned to IP address 76.138.92.28. The subscriber is James MATHEWS at service address 7043 Stout Rd. Germantown, TN. This address is at a municipal boundary and may also be referred to as 7043 Stout Rd. Memphis, TN.

35. On December 29, 2022, I examined two of the eight files referenced in paragraph 31.

- a. Observations of file name: (Pthc) 4yo Susan.mpg. This is a video file approximately 5 minutes long. The video shows a prepubescent girl lying down with her genitals exposed to the camera. An adult's hand touches the victim's genitals, rubs between her labia, and penetrates her anus with a finger.
- b. Observations of file name: (Pthc) Lily 10Yo Takes It Fully - 8m39S.avi. This is a video file approximately 8 minutes, 39 seconds long. The video shows a prepubescent girl lying down with her genitals exposed to the camera. An adult male performs oral-genital intercourse on the victim. The adult male also inserts his penis into the victim and performs genital-genital intercourse.

36. On January 11, 2022, I examined three of the eight files referenced in paragraph 32.

- a. Observations of file name: !!! NEW !!! 2010 kait 5yo - chunk2 FK pthc best.avi. This is a video file approximately 1 minute, 25 seconds long. The video shows a

prepubescent victim who appears to be a toddler. Her genitals are exposed to the camera and an apparent adult male performs genital-genital intercourse on the victim.

- b. Observations of file name: PTHC - beauty-cumshot 3yo THIS ROCKS pedo child toddler incest 2yo 4yo 5yo 6yo 7yo 8yo babyj vicky laura jenny sofie fdsa hussyfan russian korea.mpg. This is a video file approximately 6 minutes, 37 seconds long. The video shows a nude prepubescent victim who appears to be an infant/toddler. The victim is lying near a diaper that appears previously worn. An adult male performs various sexual acts on the victim including oral-genital intercourse, attempted genital-genital intercourse, and inserts his erect penis into the victim's mouth. The male ejaculates onto the genitals and abdomen of the infant/toddler who then smears and claps the semen around her body.
- c. Observations of file name: pthc Pedoland Frifam Toddler Fucking & Cumshots 3yo girl, Very Good!!.mpg. This is a video file approximately 5 minutes and 46 seconds long. This video show multiple clips of prepubescent victims, some of whom appear to be infants/toddlers. Some of the scenes included on this file are of an adult male performing genital-genital intercourse on a prepubescent victim who is bound, an adult male straddling an infant/toddler while masturbating, and an infant/toddler who appears to be crying and then whose face is ejaculated on.

37. On May 15, 2023, I visited 7043 Stout Rd. Memphis, TN to determine if internet service subscriber James MATHEWS would be willing to speak with me regarding this investigation. MATHEWS agreed to speak with HSI Agents and invited me into his home along with Special Agent Brooks Sample and Computer Forensic Analyst (CFA) Anthony Blaylock. I

advised MATHEWS he was not under arrest and he was free to walk away or terminate the encounter at any time. MATHEWS spoke with HSI Agents and provided written consent for all electronics in his home to be examined. HSI Agents did not locate information which suggested he had violated child pornography statutes or had any guilty knowledge of same. HSI Agents did not locate any indications of child pornography on his computer located in his master bedroom.

38. During HSI Agents' conversation with MATHEWS, he stated Joshua MORRISS is his adult daughter's boyfriend and he stays in an upstairs bedroom. MATHEWS stated there was a computer in the bedroom MORRISS stays in. MATHEWS stated he owns the house located at 7043 Stout Rd. and all of its contents. During this time, CFA Blaylock proceeded to conduct field examinations of additional electronic devices to identify evidence of child pornography.

39. MATHEWS called MORRISS who came downstairs. HSI Agents identified themselves and asked if he would be willing to speak with them. MORRISS sat down at the kitchen table and agreed to speak with HSI Agents. I advised MORRISS he was not under arrest and he was free to walk away or terminate the encounter at any time.

40. MORRISS admitted to downloading and possessing child pornography. MORRISS stated he downloaded child pornography from FRESHMEAT.IO, a torrent site wherein files may be downloaded and distributed via P2P file sharing. MORRISS stated he also downloaded child pornography from other sources using Tor aka Onion Router. Tor allows computer operators to access and navigate what is commonly referred to as the "Dark Web."

41. I displayed to MORRISS three sanitized screenshots of child pornography movies referenced in paragraphs 31 and 32. The screenshots were sanitized insofar as faces were masked, genitals and genital regions were masked, and the chest areas of female children were masked. MORRISS stated he recognized one of the three screenshots (identified as file name: PTHC -

beauty-cumshot 3yo THIS ROCKS pedo child toddler incest 2yo 4yo 5yo 6yo 7yo 8yo
babyj vicky laura jenny sofie fdsa hussyfan russian korea.mpg.).

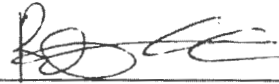
42. MORRISS stated he had a collection of child pornography saved in a folder on the computer in the bedroom which he stayed in. I asked if he would be willing to show me the folder on the computer and he agreed. MORRISS provided the password to the computer and showed me and CFA Blaylock how to navigate to folders on the computer which were said to contain child pornography. During this process, I observed thumbnail images which appeared to show nude pre-pubescent children and thumbnail images which appeared to show close-up images of vulvas. I advised MORRISS and MATHEWS that I was seizing the computer (SUSPECT DEVICE). HSI agents transported SUSPECTED DEVICE to HSI Memphis where it is currently located in secure storage.

43. After examining the files discussed in paragraphs 35 and 36, I determined that they constitute child pornography as defined in 18 U.S.C. § 2256. After speaking with MORRISS and viewing the thumbnails noted in paragraph 41, I determined the thumbnails probably constitute child pornography as defined in 18 U.S.C. § 2256.

CONCLUSION

44. I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A on SUSPECT DEVICE described in Attachment A. I, therefore, request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted,



Benjamin W. Grant
Special Agent, HSI

Pursuant to Federal Rule of Criminal Procedure 41(d)(3), the undersigned judicial officer has on this date considered information communicated by ☒ telephone or ☐ other reliable electronic means or ☐ both, in reviewing and deciding whether to issue a search warrant. In doing so, this judicial officer has placed the affiant under oath and has confirmed by speaking personally with the affiant on the telephone ☒ that the signatures on the search warrant application and affidavit are those of the affiant or ☐ that the affiant has authorized the placement of the affiant's signatures on the application and affidavit, the documents received by the judicial officer are a correct and complete copy of the documents submitted by the affiant, and the information contained in the search warrant application and affidavit are true and correct to the best of the affiant's knowledge.

Subscribed and sworn to before me on June 1, 2023.

s/Annie T. Christoff

Honorable Annie T. Christoff
United States Magistrate Judge
Western District of Tennessee